DAVID CRAIG

STATE REPRESENTATIVE

CHAIRMAN, ASSEMBLY COMMITTEE ON FINANCIAL INSTITUTIONS

Assembly Committee on State Affairs and Government Operations Public Hearing
10 February 2016
Assembly Bill 845
Representative David Craig, 83rd Assembly District

Chairman Swearingen and Committee Members,

Thank you for hearing testimony on Assembly Bill 845.

Currently, the law enforcement community is dealing with the rapid progression and expansion of surveillance technology. In response, the legislature has recently acted on reigning in technologies like drones, cell phone trackers other tracking devices. Unfortunately, the rapid onset of technologies that have the capability of collecting massive amounts of personal data pose Constitutional issues that the legislature has a duty to review. These devices include but are not limited to: Automatic License Plate Readers (ALPRs) which automatically collect and store information on millions of vehicle locations across the state of individuals never charged with a crime; Stingray devices, which mimic cell towers, allowing the collection location data, phone numbers dialed or received, and, according to media accounts, possibly voice and text communication content (we unfortunately don't know what exactly they can do, since this information is proprietary and beyond public view); and finally some departments in other states use infrared and thermal imaging devices that allow the tracking of movements through walls. According to media accounts, departments in some states even use vans outfitted with x-ray devices enabling them to drive around cities taking information about the interiors of buildings and vehicles. This rapid advancement of technology merits a level of legislative oversight not currently in existence.

To achieve both legislative access to information and to ensure the good conduct of state agents, this bill creates a legislative committee that has access to information on any new surveillance technology employed by law enforcement in Wisconsin, information relating to transfers of military equipment from the federal government to local law enforcement and to information related to closed John Doe proceedings. Under the bill, this committee maintains inherent subpoena power to ensure the free flow of information to committee members. Despite the claims of some, this bill does not give the legislature the power to prevent equipment acquisition by law enforcement, it merely requires information on these acquisitions be reported to the Committee. The subpoena power granted by the legislation is not a wholly new power but rather a simplification of the subpoena power already possessed by each legislative committee.

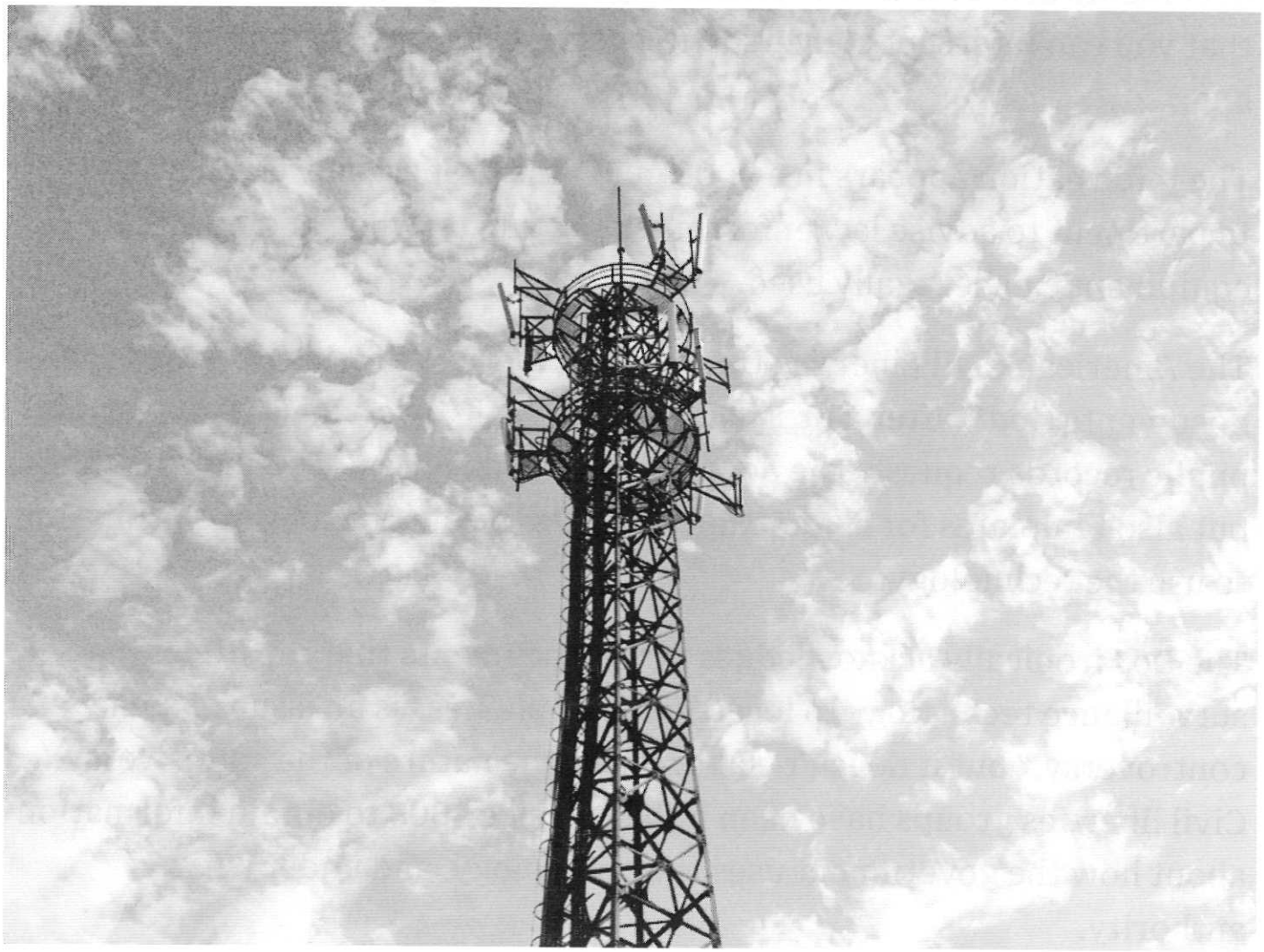
This legislation is an important step towards restoring the legislature's ability to form policy on matters of public concern and for that reason I appreciate your hearing of this bill today and I look forward to answering any questions you may have.

POST OFFICE BOX 8952 • MADISON, WI 53708-8952
(608) 266-3363 • TOLL-FREE: (888) 534-0083 • FAX: (608) 282-3683 • REP.CRAIG@LEGIS.WI.GOV

SUBSCRIBE

KIM ZETTER SECURITY 10.28.15 3:00 PM

TURNS OUT POLICE STINGRAY SPY TOOLS CAN INDEED RECORD CALLS



GETTY IMAGES

THE FEDERAL GOVERNMENT has been fighting hard for years to hide details about its use of so-called stingray surveillance technology from the public.

The surveillance devices simulate cell phone towers in order to trick nearby mobile phones into connecting to them and revealing the phones'

locations.

Now documents recently obtained by the ACLU confirm long-held suspicions that the controversial devices are also capable of recording numbers for a mobile phone's incoming and outgoing calls, as well as intercepting the content of voice and text communications. The documents also discuss the possibility of flashing a phone's firmware "so that you can intercept conversations using a suspect's cell phone as a bug."

The information appears in a 2008 guideline prepared by the Justice Department to advise law enforcement agents on when and how the equipment can be legally used.

The American Civil Liberties Union of Northern California obtained the documents (.pdf) after a protracted legal battle involving a two-year-old public records request. The documents include not only policy guidelines, but also templates for submitting requests to courts to obtain permission to use the technology.

The DoJ ironically acknowledges in the documents that the use of the surveillance technology to locate cellular phones "is an issue of some controversy," but it doesn't elaborate on the nature of the controversy. Civil liberties groups have been fighting since 2008 to obtain information about how the government uses the technology, and under what authority.

Local law enforcement agencies have used the equipment numerous times in secret without obtaining a warrant and have even deceived courts about the nature of the technology to obtain orders to use it. And they've resorted to extreme measures to prevent groups like the ACLU from obtaining documents about the technology.

Stingrays go by a number of different names, including cell-site simulator, triggerfish, IMSI-catcher, Wolfpack, Gossamer, and swamp box, according

to the documents. They can be used to determine the location of phones, computers using open wireless networks, and PC wireless data cards, also known as air cards.

The devices, generally the size of a suitcase, work by emitting a stronger signal than nearby towers in order to force a phone or mobile device to connect to them instead of a legitimate tower. Once a mobile device connects, the phone reveals its unique device ID, after which the stingray releases the device so that it can connect to a legitimate cell tower, allowing data and voice calls to go through. Assistance from a cell phone carrier isn't required to use the technology, unless law enforcement doesn't know the general location of a suspect and needs to pinpoint a geographical area in which to deploy the stingray. Once a phone's general location is determined, investigators can use a handheld device that provides more pinpoint precision in the location of a phone or mobile device—this includes being able to pinpoint an exact office or apartment where the device is being used.

In addition to the device ID, the devices can collect additional information.

"If the cellular telephone is used to make or receive a call, the screen of the digital analyzer/cell site simulator/triggerfish would include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected)," the documents note.

In order to use the devices, agents are instructed to obtain a pen register/trap and trace court order. Pen registers are traditionally used to obtain phone numbers called and the "to" field of emails, while trap and trace is used to collect information about received calls and the "from" information of emails.

When using a stingray to identify the specific phone or mobile device a suspect is using, "collection should be limited to device identifiers," the

DoJ document notes. "It should not encompass dialed digits, as that would entail surveillance on the calling activity of all persons in the vicinity of the subject."

The documents add, however, that the devices "may be capable of intercepting the contents of communications and, therefore, such devices must be configured to disable the interception function, unless interceptions have been authorized by a Title III order."

Title III is the federal wiretapping law that allows law enforcement, with a court order, to intercept communications in real time.

Civil liberties groups have long suspected that some stingrays used by law enforcement have the ability to intercept the content of voice calls and text messages. But law enforcement agencies have insisted that the devices they use are not configured to do so. Another controversial capability involves the ability to block mobile communications, such as in war zones to prevent attackers from using a mobile phone to trigger an explosive, or during political demonstrations to prevent activists from organizing by mobile phone. Stingray devices used by police in London have both of these capabilities, but it's not known how often or in what capacity they have been used.

The documents also note that law enforcement can use the devices without a court order under "exceptional" circumstances. Most surveillance laws include such provisions to give investigators the ability to conduct rapid surveillance under emergency circumstances, such as when lives are at stake. Investigators are then to apply for a court order within 24 hours after the emergency surveillance begins. But according to the documents, the DoJ considers "activity characteristic of organized crime" and "an ongoing attack of a protected computer (one used by a financial institution or U.S. government) where violation is a felony" to be considered an exception, too. In other words, an emergency situation could be a hack involving a financial institution.

"While such crimes are potentially serious, they simply do not justify bypassing the ordinary legal processes that were designed to balance the government's need to investigate crimes with the public's right to a government that abides by the law," Linda Lye, senior staff attorney for the ACLU of Northern California, notes in a blog post about the documents.

Another issue of controversy relates to the language that investigators use to describe the stingray technology. Templates for requesting a court order from judges advise the specific terminology investigators should use and never identify the stingray by name. They simply describe the tool as either a pen register/trap and trace device or a device used "to detect radio signals emitted from wireless cellular telephones in the vicinity of the Subject that identify the telephones."

The ACLU has long accused the government of misleading judges in using the pen register/trap and trace term—since stingrays are primarily used not to identify phone numbers called and received, but to track the location and movement of a mobile device.

Investigators also seldom tell judges that the devices collect data from all phones in the vicinity of a stingray—not just a targeted phone—and can disrupt regular cell service.

It's not known how quickly stingrays release devices that connect to them, allowing them to then connect to a legitimate cell tower. During the period that devices are connected to a stingray, disruption can occur for anyone in the vicinity of the technology.

Disruption can also occur from the way stingrays force-downgrade mobile devices from 3G and 4G connectivity to 2G if they are being used to intercept the concept of communications.

In order for the kind of stingray used by law enforcement to work for this purpose, it exploits a vulnerability in the 2G protocol. Phones using 2G

don't authenticate cell towers, which means that a rogue tower can pass itself off as a legitimate cell tower. But because 3G and 4G networks have fixed this vulnerability, the stingray will jam these networks to force nearby phones to downgrade to the vulnerable 2G network to communicate.

"Depending on how long the jamming is taking place, there's going to be disruption," Chris Soghoian, chief technology for the ACLU has told WIRED previously. "When your phone goes down to 2G, your data just goes to hell. So at the very least you will have disruption of internet connectivity. And if and when the phones are using the stingray as their only tower, there will likely be an inability to receive or make calls."

Concerns about the use of stingrays is growing. Last March, Senator Bill Nelson (D—Florida) sent a letter to the FCC calling on the agency to disclose information about its certification process for approving stingrays and any other tools with similar functionality. Nelson asked in particular for information about any oversight put in place to make sure that use of the devices complies with the manufacturer's representations to the FCC about how the technology works and is used.

Nelson also raised concerns about their use in a remarkable speech on the Senate floor. The Senator said the technology "poses a grave threat to consumers' cellphone and Internet privacy," particularly when law enforcement agencies use them without a warrant.

The increased attention prompted the Justice Department this month to release a new federal policy on the use of stingrays, requiring a warrant any time federal investigators use them. The rules, however, don't apply to local police departments, which are among the most prolific users of the technology and have been using them for years without obtaining a warrant.

#CELLPHONES #GOVERNMENT SURVEILLANCE #SPYING #STINGRAYS

VIEW COMMENTS

SPONSORED STORIES

POWERED BY OUTBRAIN

MORE SECURITY

The Atlantic

The NYPD Is Using Mobile X-Ray Vans to Spy on Unknown Targets

New York City won't reveal how often cops bombard places, vehicles, or people with radiation—or if there are health risks for residents.

Stephanie Keith / Reuters

CONOR FRIEDERSDORF

OCT 19, 2015 | POLITICS

TEXT SIZE

Dystopian truth is stranger than dystopian fiction.

In New York City, the police now maintain an unknown number of military-grade vans outfitted with X-ray radiation, enabling cops to look through the walls of buildings or the sides of trucks. The technology was used in

Afghanistan before being loosed on U.S. streets. Each X-ray van costs an estimated $729,000 to $825,000.

The NYPD will not reveal when, where, or how often they are used.

"I will not talk about anything at all about this," New York Police Commissioner Bill Bratton told a journalist for the *New York Post* who pressed for details on the vans. "It falls into the range of security and counter-terrorism activity that we engage in."

He added that "they're not used to scan people for weapons."

Here are some specific questions that New York City refuses to answer:

- How is the NYPD ensuring that innocent New Yorkers are not subject to harmful X-ray radiation?
- How long is the NYPD keeping the images that it takes and who can look at them?
- Is the NYPD obtaining judicial authorization prior to taking images, and if so, what type of authorization?
- Is the technology funded by taxpayer money, and has the use of the vans justified the price tag?

Those specifics are taken from a New York Civil Liberties Union court filing. The legal organization is seeking to assist a lawsuit filed by *Pro Publica* journalist Michael Grabell, who has been fighting New York City for answers about X-ray vans for 3 years.

"ProPublica filed the request as part of its investigation into the proliferation of security equipment, including airport body scanners, that expose people to ionizing radiation, which can mutate DNA and increase the risk of cancer," he explained. (For fear of a terrorist "dirty bomb," America's security apparatus is exposing its population to radiation as a matter of course.)

A state court has already ruled that the NYPD has to turn over policies, procedures, and training manuals that shape uses of X-rays; reports on past deployments; information on the costs of the X-ray devices and the number of vans purchased; and information on the health and safety effects of the technology. But New York City is fighting on appeal to suppress that information and more, as if it is some kind of spy agency rather than a municipal police department operating on domestic soil, ostensibly at the pleasure of city residents.

Its insistence on extreme secrecy is part of an alarming trend. The people of New York City are effectively being denied the ability to decide how they want to be policed.

"Technologies—from x-ray scanners to drones, automatic license plate readers that record license plates of cars passing by, and 'Stingrays' that spy on nearby cell phones by imitating cell phone towers—have brought rapid advances to law enforcement capacity to monitor citizens," the NYCLU notes. "Some of these new technologies have filtered in from the battlefields into the hands of local law enforcement with little notice to the public and with little oversight. These technologies raise legitimate questions about cost, effectiveness, and the impact on the rights of everyday people to live in a society free of unwarranted government surveillance."

For all we know, the NYPD might be bombarding apartment houses with radiation while people are inside or peering inside vehicles on the street as unwitting passersby are exposed to radiation. The city's position—that New Yorkers have no right to know if that is happening or not—is so absurd that one can hardly believe they're taking it. These are properly political questions. And it's unlikely a target would ever notice. "Once equipped, the van—which looks like a standard delivery van—takes less than 15 seconds to scan a vehicle," *Fox News* reported after looking at X-ray vans owned by the

federal government. "It can be operated remotely from more than 1,500 feet and can be equipped with optional technology to identify radioactivity as well."

In her ruling, Judge Doris Ling-Cohan highlights the fact that beyond the privacy questions raised by the technology are very real health and safety concerns. She writes:

> Petitioner states in his affidavit, and respondent does not dispute, that: backscatter technology, previously deployed in European Union airports, was banned in 2011, because of health concerns; an internal presentation from American Science and Engineering, Inc., the company that manufactures the vans, determined that the vans deliver a radiation dose 40 percent larger than delivered by a backscatter airport scanner; bystanders present when the van is in use are exposed to the radiation that the van emits... moreover, petitioner maintains, and it is not disputed by the NYPD, that 'there may be significant health risks associated with the use of backscatter x-ray devices as these machines use ionizing radiation, a type of radiation long known to mutate DNA and cause cancer.
>
> Finally, petitioner states, again without dispute, that, on August 2011, the United States Customs and Border Protection Agency, which used the vans to scan vehicles crossing into and out of the United States, despite repeated testing and analysis of the amount of radiation emitted by such devices, nevertheless, prohibited continued use of the vans to scan occupied vehicles, until approval was granted by the United States Custom and Border Protection Radiation and Safety Committee...

And since the technology can see through clothing, it is easy to imagine a misbehaving NYPD officer abusing it if there are not sufficient safeguards in place. Trusting the NYPD to choose prudent, sufficient safeguards under cover of secrecy is folly. This is the same department that spent 6 years conducting surveillance on innocent Muslims Americans in a program so unfocused that it produced zero leads—and that has brutalized New York City protestors on numerous occasions. Time and again it's shown that outside oversight is needed.

Lest readers outside New York City presume that their walls still stand between them and their local law enforcement agency, that isn't necessarily the case. Back in January, in an article that got remarkably little attention, *USA Today* reported the following:

> At least 50 U.S. law enforcementagencies have secretly equipped their officers with radar devices that allow them to effectively peer through the walls of houses to see whether anyone is inside, a practice raising new concerns about the extent of government surveillance. Those agencies, including the FBI and the U.S. Marshals Service, began deploying the radar systems more than two years ago with little notice to the courts and no public disclosure of when or how they would be used. The technology raises legal and privacy issues because the U.S. Supreme Court has said officers generally cannot use high-tech sensors to tell them about the inside of a person's house without first obtaining a search warrant. The radars work like finely tuned motion detectors, using radio waves to zero in on movements as slight as human breathing from a distance of more than 50 feet. They can

detect whether anyone is inside of a house, where they are and whether they are moving.

The overarching theme here is a law enforcement community that has never seen a technology that causes it to say, "We'd better ask if the public wants us to use this or not."

Instead, the usual protocol is not only to adopt new technology without permission—regardless of the privacy, health and safety, or moral questions that it raises—but to keep having done so a secret as long as possible, and to hide the true nature of the technology in question even after the public has been alerted to its existence. The fact that this pattern has held in regards to a device that can look through walls while emitting radiation on the streets of New York City raises questions including "What's next?" "What else don't we know about?" and "Will any technology on the military-to-police pipeline ever cause cops to ask permission first?"

ABOUT THE AUTHOR

CONOR FRIEDERSDORF is a staff writer at *The Atlantic,* where he focuses on politics and national affairs. He lives in Venice, California, and is the founding editor of The Best of Journalism, a newsletter devoted to exceptional nonfiction.

Twitter Email

◀ previous next story ▶

STATE OF WISCONSIN
DEPARTMENT OF JUSTICE

BRAD D. SCHIMEL
ATTORNEY GENERAL

Andrew C. Cook
Deputy Attorney General

114 East, State Capitol
P.O. Box 7857
Madison, WI 53707-7857
608/266-1221
TTY 1-800-947-3529

To: **Assembly Committee on State Affairs & Government Operations**

From: **Attorney General Brad Schimel**
Wisconsin Department of Justice

Date: **February 10, 2016**

Subject: **Opposition Assembly Bill 845**

Thank you Chairman Swearingen and committee members for the opportunity to present written testimony to you in opposition to Assembly Bill 845.

As Attorney General, I strongly oppose Assembly Bill 845 and share the concerns submitted in the opposition memo from the Wisconsin Sheriffs and Deputy Sheriffs Association, Badger State Sheriffs' Association, County Law Enforcement Professionals of Wisconsin, Wisconsin Chiefs of Police Association, and the Wisconsin Professional Police Association.

First and foremost, the proposed law is unnecessary as there is no evidence of a crisis in Wisconsin involving law enforcement using any tools to track criminals. The courts appropriately serve as the guardian of our citizens' right to privacy under the State Constitution and U.S. Constitution and Assembly Bill 845 does nothing to change that fact.

Second, as written, the bill would compel law enforcement to compromise existing and ongoing criminal investigations. If the bill moves forward, it should be amended to include an exemption for ongoing investigations which would be impacted by disclosure to the legislative committee on the oversight of law enforcement and investigation.

Third, and most troubling, the bill will actually serve the interests of criminals by allowing them to evade accountability and punishment by exposing techniques used by the police that may be developed in the future that are both Constitutional and effective.

Fourth, Assembly Bill 845 will disrupt the effective relationship between state and local law enforcement agencies and their federal partners. The Division of Criminal Investigation at the Wisconsin Department of Justice, in addition to nearly every state and local law enforcement agency, work jointly in task forces with federal agencies such as the Federal Bureau of Investigation (FBI), Drug Enforcement Agency (DEA), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and Department of Homeland Security (DHS). The Wisconsin legislature does not have authority over these federal agencies, nor would any of the agencies subject themselves to the

jurisdiction of the legislative committee on the oversight of law enforcement and investigation. Yet Assembly Bill 845 would disrupt these relationships because state and local law enforcement agencies would be subject to the subpoena power of the legislative committee on the oversight of law enforcement and investigation which will likely cause these task forces to cease operation and for local law enforcement to have no role in stopping criminal activity that may be occurring in its jurisdiction.

Last, Assembly Bill 845 allows the legislative committee on the oversight of law enforcement and investigation to stop law enforcement from investing in necessary software upgrades or new electronic hardware in light of the fact that the proposal calls for the review of proposed contracts. Many software companies include trade secret language in their contracts that is confidential and will not do business with law enforcement if it will risk exposing a trade secret, the contract terms, or a description of the technology itself that is the subject of the contract.

Again, thank you for your consideration of Assembly Bill 885 and please feel free to contact me with any questions.

TO:	Representative Rob Swearingen, Chair Representative David Craig, Vice-Chair Members, Assembly Committee on State Affairs & Government Operations
FROM:	Wisconsin Sheriffs and Deputy Sheriffs Association (WS&DSA) Badger State Sheriffs' Association (BSSA) County Law Enforcement Professionals of Wisconsin (CLEPW) Wisconsin Chiefs of Police Association (WCPA) Wisconsin Professional Police Association (WPPA)
DATE:	February 10, 2015
RE:	**Opposition to 2015 Assembly Bill 845/Senate Bill 639**

Representing the vast majority of Wisconsin's law enforcement community, the organizations listed above submit this memorandum to collectively express their **OPPOSITION to AB 845, which threatens to comprise the state's public records law, local control, and law enforcement investigations.**

Current Law

The operations of any local law enforcement agency in Wisconsin is subject to numerous layers of oversight by duly-elected officials that must answer to the voters of any community. The use of a device and technology by a law enforcement agency to conduct surveillance on a person suspected of a crime is generally approved by a circuit court judge to ensure that the private constitutional rights of privacy and due process are properly afforded. Additionally, an agency's acquisition and use of technology requires the specific approval of the governing body of a municipality or county. The same is also true for a law enforcement agency's acquisition of any weapons, equipment, or armaments from a federal military unit.[1]

Assembly Bill 845

AB 845 generally creates a legislative committee to oversee issues related to the acquisition and use of surveillance technology by a law enforcement agency. So that it may carry out the responsibilities contemplated by the bill, AB 845 provides the committee with unique subpoena and arrest powers, along with access to investigatory records otherwise protected from disclosure by statute or a court order.

---

[1] Civilian law enforcement agencies can acquire surplus military equipment from the federal government through the 1033 Program, which was created by the National Defense Authorization Act of Fiscal Year 1997. In order to acquire resources through this program, state and local officials are required to maintain an "audit trail" for each item and conduct periodic inventory checks to ensure that federal properties have not been sold, stolen or misappropriated. In May of 2015, President Obama issued Executive Order 13688 to significantly restrict the equipment that a local law enforcement agency may receive through the program.

1. **The unique subpoena powers provided to the oversight committee by AB 845 raise concerns about the committee's autonomy and its duty to comply with the state public records law.**

Under current law, the attendance of witnesses and production of evidence before any committee of the legislature may be procured by subpoenas signed by a presiding officer and chief clerk of the senate or assembly.[2] Current law also designates the chief clerk of either house to produce and maintain the official legislative record.[3] AB 845 specifically provides that a subpoena issued by this committee does not require the signature of a presiding officer or a chief clerk, and that the subpoena shall be returned to the committee chairperson after it is served. While it appears that these provisions require the committee chairperson to maintain a subpoena issued by the committee as a record that is subject to disclosure under the state's public records law,[4] that is unclear, as is the matter of whether AB 845 provides enough oversight for the committee itself with respect to its exercise of those special subpoena powers granted by the bill.[5]

2. **Information released by the oversight committee pursuant to the public records law will likely compromise ongoing criminal investigations.**

While AB 845 provides that a subpoena issued by the oversight committee may not compel the production or disclosure of personal identifying information of uncharged persons or organizations or of trade secrets, the bill includes no provision to safeguard the subpoena itself from disclosure,[6] or of information contained therein.[7] As such, information identifying the municipality, county, law enforcement agency, or public official that is the subject of a subpoena issued by this oversight committee, or some description of the information sought by a subpoena, will have to be made public. While the law enforcement groups listed in this memorandum offer no position as to whether the bill should create additional exemptions under the public records law, they are concerned about the extent to which the release of information contained in a subpoena might compromise an ongoing criminal investigation. It is not unreasonable to imagine a scenario in which the perpetrator of a crime alters their behavior to evade detection after learning through media reports about specific investigative tools being utilized by law enforcement in their immediate area.

3. **AB 845 is ambiguous regarding the oversight committee's obligations under the public records law, and will result in litigation as a result.**

Under the public records law, an authority may deny the release of information and records sought by a records request after applying a balancing test that weighs the public interest in disclosure against the public interest in nondisclosure.[8] The use of that balancing test has been the source of

---

[2] Wis. Stat. § 13.31.

[3] Wis. Stat. § 13.16.

[4] A subpoena itself constitutes a record, unless protected from disclosure by a secrecy order issued by a circuit court judge under Wis. Stat. § 928.26, or it falls under one of the specific public records law exemptions under Wis. Stat. § 19.36.

[5] Interestingly, SB 639 provides the oversight committee with access to investigatory records currently made unavailable by the law enforcement records exemption found in 19.36(2), as well as those protected by a secrecy order issued by a circuit court judge in John Doe proceedings under Wis. Stat. § 928.26.

[6] *See infra* note 4.

[7] Under Wis. Stat. § 19.36(6), if part of the record is disclosable, that part must be disclosed. Also, an authority is not relieved of the duty to redact non-disclosable portions just because the authority believes that redacting confidential information is burdensome. *Osborn v. Bd. of Regents*, 2002 WI 83, ¶ 46, 254 Wis. 2d 266, ¶ 46, 647 N.W.2d 158, ¶ 46.

[8] *Journal Co. v. County Ct.*, 43 Wis. 2d 297, 168 N.W.2d at 839 (1969). The custodian must identify potential reasons for denial, based on public policy considerations indicating that denying access is or may be appropriate. *Id.* Those factors

considerable litigation.[9] While the oversight committee created by AB 845 could conceivably apply the balancing test and determine that the public policy considerations against releasing information connected with the committee's work or a subpoena issued by it outweigh the public interest in disclosure, special consideration ought to be given to the issue. In not specifically addressing the extent to which information may be released by the oversight committee under the public records law, AB 845 is likely to cause significant confusion among elected officials, law enforcement agencies, legislators serving on the oversight committee, and the public alike, resulting in additional litigation regarding the committee's obligations under the public records law.

4. The only way the oversight committee created by AB 845 can fulfill is statutory duty to review the statewide law enforcement use of surveillance devices and technology when it is enacted is to subpoena every law enforcement agency in Wisconsin.

In the event AB 845 was enacted into law, it provides that the law enforcement oversight committee is to review the current use of technology services or electronic devices by a law enforcement agency. Notably, the bill does not provide the committee with any means other than its subpoena powers to obtain information as to that use of surveillance resources. In other words, the only way the oversight committee could discern under the bill which law enforcement agencies in Wisconsin are already using some device or technology that is or may be used for the purpose of surveillance is by issuing a subpoena to every agency in the state.[10] The burdens this creates for local governments, law enforcement agencies, the oversight committee itself are significant.

5. AB 845 creates other undue burdens upon local governments and undermines the principles of local control.

One provision included in AB 845 appears to only require an agency to <u>notify</u> the oversight committee of the proposed acquisition by a law enforcement agency of a new surveillance device or technology service before the acquisition takes place. Another provision in AB 845, however, empowers the committee to review "any proposed acquisition" of a device or service. Under the longstanding judicial precedents governing statutory interpretation, AB 845 must be read to require the oversight committee to perform some degree of review of a new surveillance resource

---

must be weighed against public interest in disclosure. *Id.* Specific policy reasons, rather than mere statements of legal conclusion or recitation of exemptions, must be given. *Pangman & Assocs. v. Zellmer*, 163 Wis. 2d 1070, 1084, 473 N.W.2d 538, 543-44 (Ct. App. 1991); *Vill. of Butler v. Cohen*, 163 Wis. 2d 819, 824-25, 472 N.W.2d 579, 581 (Ct. App. 1991). Generally, there are no blanket exemptions from release, and the balancing test must be applied with respect to each individual record. *Milwaukee Journal Sentinel v. Dep't of Admin.*, 2009 WI 79, ¶ 56, 319 Wis. 2d 439, ¶ 56, 768 N.W.2d 700, ¶ 56. The records custodian must consider all relevant factors to determine whether permitting record access would result in harm to the public interest that outweighs the legislative policy recognizing the strong public interest in allowing access. Wis. Stat. § 19.35(1)(a). The balancing test is a fact-intensive inquiry that must be performed on a case-by-case basis. *Kroeplin v. Wis. Dep't Natural Res.*, 2006 WI App 227, ¶ 37, 297 Wis. 2d 254, ¶ 37, 725 N.W.2d 286, ¶ 37. A records custodian is not expected to examine a public records request "in a vacuum." *Seifert v. Sch. Dist. of Sheboygan Falls*, 2007 WI App 207, ¶ 31, 305 Wis. 2d 582, ¶ 31, 740 N.W.2d 177, ¶ 31. The public records law contemplates examination of all relevant factors, considered in the context of the particular circumstances. *Id.* In other words, the records custodian must determine whether the surrounding circumstances create an exceptional case not governed by the strong presumption of openness. *Hempel v. City of Baraboo*, 2005 WI 120, ¶ 63, 284 Wis. 2d 162, ¶ 63, 699 N.W.2d 551, ¶ 63. An "exceptional case" exists when the circumstances are such that the public policy interests favoring nondisclosure outweigh the public policy interests favoring disclosure, notwithstanding the strong presumption favoring disclosure. *Id.* The identity of the requester and the purpose of the request are not part of the balancing test. *See Kraemer Bros., Inc. v. Dane County*, 229 Wis. 2d 86, 102, 599 N.W.2d 75, 83 (Ct. App. 1999).

[9] *Id.*

[10] There are nearly 400 law enforcement agencies in Wisconsin.

before a law enforcement agency may acquire it.[11] As such, the bill is highly likely to foster a significant degree of uncertainty for law enforcement agencies and local units of government, creating significant burdens for both, including an unnecessary delay in the use of surveillance resources that might be critically needed to detect and thwart ongoing criminal activity.

Additionally, AB 845 requires the oversight committee to "review for appropriateness" the proposed transfer of "military weapons, surveillance equipment, or armaments" from the federal military, before the transfer takes place. This requirement will cause unnecessary delays that could impair ongoing criminal investigations by law enforcement and undermine the authority of the local governments that have already authorized the transfer.[12] Also, because of the broad language utilized in this broad mandate, AB 845 would appear to unreasonably require that a local government's acquisition of any federal military resources, even ammunition, be specifically approved by the oversight committee prior to a local government's receipt and use of those items.

6. Additional AB 845 concerns.

a. The oversight committee fails to include some law enforcement representation, even in an *ex officio* capacity.

b. The bill provisions requiring the oversight committee to review any contract for the acquisition of any surveillance resource and that those contracts themselves must contain a provision allowing the committee to review the agreement are both completely superfluous, unnecessary, and a further subjugation of the role of duly-elected municipal and county officials by the state legislature.

c. The bill offers no guidance as to whether updates in surveillance resources currently available to and in use by law enforcement agencies require oversight committee review.

d. The bill ties law enforcement's hands by failing to provide for any good-faith allowance for the acquisition or use of any device or technology that might be needed under swiftly-emergent or exigent circumstances to quickly react to an ongoing criminal investigation.

e. The bill fails to also provide for any penalties in the event that protected or confidential information is divulged by any member of the oversight committee. Without any enforcement mechanism, AB 845 inadequately protects against the release of information that could compromise the integrity of an ongoing criminal investigation, John Doe proceeding, or the proprietary corporate interests of a manufacturer of emerging technologies with criminal justice benefits.

LAW ENFORCEMENT GROUP CONTACTS:
WS&DSA: Caty McDermott/R.J. Pirlot - (608) 258-9506
BSSA: Dean Meyer, Executive Director - (715) 415-2412
CLEPW: Ramie Zelenkova of Hubbard Wilson & Zelenkova, LLC - (608)255-0566
WCPA: Chief Greg Leck - (608) 973-4057; Chief Steve Riffel - (920) 47-7955; Alice O'Connor - (608) 225-9391
WPPA: Jim Palmer, Executive Director - (608) 273-3840

---

[11] *Wood County v. Board of Vocational, Technical & Adult Education*, 60 Wis. 2d 606, 211 N.W.2d 617 (1973) (holding that the court can only attempt to construe a statute so that all parts have a function and meaning).
[12] *See infra* note 1.